Fast Space Optimal Leader Election in Population Protocols*

Leszek Gąsieniec Grzegorz Stachowiak

Abstract

The model of *population protocols* refers to the growing in popularity theoretical framework suitable for studying *pairwise interactions* within a large collection of simple indistinguishable entities, frequently called *agents*. In this paper the emphasis is on the space complexity in fast *leader election* via population protocols governed by the *random scheduler*, which uniformly at random selects pairwise interactions within the population of n agents.

The main result of this paper is a new fast and space optimal leader election protocol. The new protocol utilises $O(\log^2 n)$ parallel time (which is equivalent to $O(n \log^2 n)$ sequential pairwise interactions), and each agent operates on $O(\log \log n)$ states. This double logarithmic space usage matches asymptotically the lower bound $\frac{1}{2} \log \log n$ on the minimal number of states required by agents in any leader election algorithm with the running time $o(\frac{n}{\text{polylog } n})$, see [6].

Our solution takes an advantage of the concept of phase clocks, a fundamental synchronisation and coordination tool in distributed computing. We propose a new fast and robust population protocol for initialisation of phase clocks to be run simultaneously in multiple modes and intertwined with the leader election process. We also provide the reader with the relevant formal argumentation indicating that our solution is always correct, and fast with high probability.

Contact author:
Leszek A Gąsieniec
Department of Computer Science
University of Liverpool
Email: L.A.Gasieniec@liverpool.ac.uk

*This work is sponsored in part by the University of Liverpool initiative Networks Sciences and Technologies (NeST) and by the Polish National Science Centre grant DEC-2012/06/M/ST6/00459.

1 Introduction

The model of *population protocols* adopted in this paper was introduced in the seminal paper of Angluin *et al.* [2]. Their model provides a universal theoretical framework for studying pairwise interactions within a large collection of anonymous (indistinguishable) entities, very often referred to as *agents*, equipped with limited communication and computation abilities. The agents are modelled as finite state machines. When two agents engage in a direct interaction they mutually access the contents of their local states and, on the conclusion of the encounter their states are modified according to the transition function that is an integral part of the population protocol. In the *probabilistic variant* of population protocols, considered in [2] and adopted in this paper, in each step the *random scheduler* selects a pair of agents uniformly at random. In this variant on the top of the *space complexity* determined by the maximum number of distinct states used by each agent, one is also interested in the *time complexity* of the proposed solutions. In more recent work on population protocols the emphasis is on parallel time defined as the total number of pairwise interactions leading to stabilisation divided by the size, in our case n, of the population.

A population protocol *terminates with success* if the whole population eventually stabilises (arrives at and stays indefinitely) in the final configuration of states reflecting the desired property of the solution. For example, in protocols targetting majority in the population, the final configuration corresponds to each agent being in the unique state representing the colour of the majority, see, e.g., [3, 5, 29, 30, 38]. In *leader election*, however, in the final configuration exactly one agent must conclude in the `leader` state and all others must stabilise in the `follower` state. The leader election problem received in recent years greater attention in the context of population protocols thanks to several important developments in closely related problems [18, 22]. In particular, the results from [18, 22] laid foundation for the proof that leader election cannot be solved in sublinear time with agents operating on a fixed number of states [24]. In further work [7], Alistarh and Gelashvili studied the relevant upper bound, and they proposed a new leader election protocol stabilising in time $O(\log^3 n)$ assuming $O(\log^3 n)$ states at each agent.

In a very recent work Alistarh *et al.* [6] consider a general trade-off between the number of states used by agents versus the time complexity of the stabilisation process. In particular, the authors provide a separation argument distinguishing between *slowly stabilising* population protocols which use $o(\log\log n)$ states and *rapidly stabilising* protocols requiring $O(\log n)$ states at each agent. This result nicely coincides with another fundamental observation by Chatzigiannakis *et al.* [17] which states that population protocols operating on $o(\log\log n)$ states can only cope with semilinear predicates while $O(\log n)$ states allow to compute symmetric predicates.

Our results In this paper we show that the lower bound on the space complexity in fast leader election proved in [6] is asymptotically tight. The lower bound states that any leader election algorithm with the time complexity $o(\frac{n}{\text{polylog } n})$ requires $\frac{1}{2}\log\log n$ states per agent. Here we present a new fast *leader election* algorithm which stabilises in time $O(\log^2 n)$ in populations with agents operating on $c\log\log n$ states, for a small positive constant c.

Our algorithm utilises a fast and low on space reduction of potential leaders (candidates) in the population. The reduction process is intertwined with a robust initialisation and further utilisation of *phase clocks*, a synchronisation tool developed and explored by the self-stabilising community [34]. This includes the seminal work on clock synchronisation by Arora *et al.* [8], further extension by Dolev and Welsh [21] to distributed systems prone to Byzantine faults, and related study on pulse synchronisation by Daliot *et al.* [23]. Our variant of the phase clock refers directly to the work of Angluin *et al.* [4] in which the authors propose efficient simulation of a *virtual register machine* supporting basic arithmetic operations. The simulation in [4] assumes availability of a single leader which coordinates the relevant exchange of information. In the same paper, the authors provide also some intuition behind the phase clock coordinated by a *junta* of n^ε leaders, for some small positive constant ε. In this work we formally prove that the phase clock based on junta of cardinality n^ε, for any $\varepsilon < 1$, allows to count $\Theta(\log n)$ time units

assuming a constant number of states at each agent. We also consider an extension of the phase clock allowing to compute time $\Theta(\log^c n)$, for any integer constant c. Our main result is based on rapid computation of junta of leaders followed by fast selection of a single leader, all in time $O(\log^2 n)$ and $O(\log\log n)$ states available at each agent.

Related work *Leader election* is one of the fundamental problems in distributed computing on par with other core problems in the field including *broadcasting*, *mutual-exclusion*, *consensus*, see an excellent text book by Attiya and Welch [11]. The problem was originally considered in networks with nodes having distinct labels [36], where an early work focuses on the ring topology in both in synchronous [26, 35] and asynchronous [16, 40] models. Also, in networks populated by mobile agents the leader election was studied first in networks with labeled nodes [33]. However, very often leader election is used also as a symmetry breaking mechanism enabling feasibility and coordination of more complex protocols in systems based on uniform (indistinguishable) entities. There is a large volume of work [1, 9, 10, 14, 15, 41, 42] on leader election in anonymous networks. In [41, 42] we find characterisation of message-passing networks in which leader election is feasible when nodes are anonymous. In [41], the authors study the problem of leader election in general networks under the assumption that node labels are not unique. In [25], the authors study feasibility and message complexity of leader election in rings with possibly non-unique labels, while, in [20], the authors provide solutions to a generalized leader election problem in rings with arbitrary labels. The work in [28] focuses on space requirements for leader election in unlabeled networks. In [27], the authors investigate the running time of leader election in anonymous networks where time is expressed in terms of multiple network parameters. In [19], the authors study feasibility of leader election among anonymous agents that navigate in a network in an asynchronous way. An interesting study on trade-offs between the time complexity and knowledge available in anonymous trees can be found in recent work of Glacet *et al.* [32].

Finally, a good example of recent extensive studies on the exact space complexity in related models refers to plurality consensus. In particular, in [13] Berenbrink *et al.* proposed a plurality consensus protocol for C original opinions converging in $O(\log C \cdot \log\log n)$ synchronous rounds using only $\log C + (\log\log C)$ bits of local memory. They also show a slightly slower solution converging in $O(\log n \cdot \log\log n)$ rounds using only $\log C + 4$ bits of local memory. This disproved the conjecture by Becchetti et al. [12] implying that any protocol with local memory $\log C + O(1)$ has the worst-case running time $\Omega(k)$. In [31] Ghaffari and Parter propose an alternative algorithm converging in $O(\log C \log n)$ rounds while having message and local memory sizes based on $\log C + O(1)$ bits. In addition, some work on the application of the random walk in plurality consenus protocols can be found in [12, 29].

2 Preliminaries

We consider population protocols defined on the complete graph of interactions where the *random scheduler* picks uniformly at random pairs of agents drawn from the population of size n. The agents are anonymous, i.e., they don't have identifiers. The protocol assumes all agents start in the same initial state. Our protocol utilises the classical model of population protocols [2, 4] where consecutive interactions refer to ordered pairs of agents (`responder`, `initiator`). On the conclusion of each interaction the two participating agents change their states (a, b) into (a', b') according to a *fixed deterministic transition function* denoted by $(a, b) \to (a', b')$.

We focus here on two complexity measures: (1) the *space complexity* defined as the *number of states* required by each agent, and (2) the *time complexity* reflecting the number of interactions needed to stabilise the protocol. Similarly to other recent work on population protocols, the emphasis here is on parallel time of the solution defined as the total number of interactions divided by the size of the population. In general terms, we aim at protocols formed of $O(n \cdot \text{poly}\log n)$ interactions translating to the running time $O(\text{poly}\log n)$.

Our leader election algorithm is always correct and it runs fast *with high probability (whp)*

which we define as follows. Let η be a parameter with an arbitrary value meeting our needs. An event occurs with *negligible* probability if it occurs with probability at most $n^{-\eta}$. An event occurs with high probability (whp) if it occurs with probability at least $1 - n^{-\eta}$. We say that an algorithm succeeds with high probability if we can incorporate the parameter η in the algorithm, s.t., it succeeds with probability at least $1 - n^{-\eta}$. In the case we refer to more specific maximum probability of failure p different from $n^{-\eta}$, we say whp $1 - p$. Our results are of asymptotic nature, i.e., we assume n is large enough to validate the results.

Throughout the paper in the analysis of the intermediate results and studied protocols we utilise several standard probabilistic tools including the *Union bound*, the *Chernoff bound*, the *Markov's inequality* and the *Bayes rule* which definitions can be found in any probability theory text book.

2.1 One-way epidemics

In our solution we adopt the notion of *one-way epidemic* introduced in [4]. One-way epidemic refers to the population protocol with the state space $\{0, 1\}$ and the transition rule $x, y \rightarrow max\{x, y), y$. One interprets 0's as *susceptible* agents and 1's as *infected* ones. This protocol corresponds to a simple epidemic in which transmission of the infection occurs if and only if the initiator is infected and the responder is susceptible. We will use the following theorem from [4].

Theorem 1 ([4]) *In order to conclude one-way epidemic (infect all agents) one needs* $\Theta(n \log n)$ *pairwise interactions with high probability.*

3 Phase clock revisited

In paper [4] Angluin *et al.* proposed the notion of and analysed *phase clocks* capable of counting approximately time $\Theta(\log n)$, when each agent participating in the population protocol is equipped with a constant number of states. However, the phase clocks from [4] work under the assumption of having already selected unique leader in the population. In the same paper, the authors argue (without a formal proof) that phase clocks should also work when a single leader is replaced by a *junta* of n^{ε} leaders, for some unspecified constant ε.

In this section we propose and analyse a slightly modified version of the phase clock capable of counting approximately time $\Theta(\log n)$, when each participating agent operates on a constant number of states and the junta of leaders is of cardinality $n^{1-\varepsilon}$, for any constant $\varepsilon : 0 < \varepsilon < 1$. Without loss of generality and for a technical reasons we take $\varepsilon = \frac{3}{3k+2}$, for a positive integer k.

The states of agents controlling the phase clock protocol are structured in pairs (x, b). The entry b has value `leader` for leaders in the junta and `follower` for all other agents. The entry x represents (the number of) a *phase* of an agent drawn from the set $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$, for some constant integer m. The phases can be interpreted as hours on a dial of an analogue clock. The periodic increment of phases is computed using the arithmetic modulo m which we denote here by $+_m$. We also define the maximum of two phases x, y in set $\mathbb{Z}_m$ as:

$$\max_m\{x, y\} = \begin{cases} \max\{x, y\} \text{ if } |x - y| \leq m/2 \\ \min\{x, y\} \text{ if } |x - y| > m/2 \end{cases}$$

Finally we define the *circular order* (which is not partial) on $\mathbb{Z}_m$ as $x \leq_m y$ iff $\max_m\{x, y\} = y$.

Now we are ready to formally define the transition function in our version of the phase clock

$$(x, \texttt{follower}), (y, b) \rightarrow (\max_m\{x, y\}, \texttt{follower}), (y, b)$$

and

$$(x, \texttt{leader}), (y, b) \rightarrow (\max_m\{x, y +_m 1\}, \texttt{leader}), (y, b)$$

In this paper we study phase clocks which operate in two modes: the *ordinary mode* and the *external mode*. These two modes differ in choosing pairwise interactions to the phase clock. In

the ordinary mode all interactions contribute to the actions of the phase clock. In the other mode interactions are chosen more selectively and they are arranged into *series* of n interactions in which every agent acts as the responder exactly once. In this mode we consider only *meaningful interactions* and we ignore others. The detail of how the meaningful interactions are chosen is provided after Theorem 2. In each subsequent series the initiators are chosen (by the random scheduler) at random and the order in which agents appear as responders is random too. For any of the two modes, we say the phase clock *passes through* 0 whenever its phase x is reduced in absolute terms (e.g., passes from phase 5 to phase 3).

Before we prove Theorem 2, which is the main result of this section, we consider several intermediate lemmas. In the proofs for the ordinary mode we utilise Theorem 1 showing that one-way epidemic protocol concludes after $\Theta(n \log n)$ whp. In the proofs for the external mode we need some analogue of this theorem in which interactions for phase clock operations are chosen such that they form random series of n interactions and in each series each agent acts as the responder exactly once.

Lemma 1 *One-way epidemic applied in the external mode requires $O(n \log n)$ meaningful interactions whp.*

Proof: Let v be the first infected agent. By the Chernoff bound, for any constant $c_1 > 0$ the number of meaningful interactions agent v needs to infect directly $c_1 \log n$ agents is bounded by $O(n \log n)$ whp $1 - n^{-\eta-1}$. Thus the number of infected agents after $O(n \log n)$ interactions is at least $c_1 \log n$ whp $1 - n^{-\eta-1}$. Also by the Chernoff bound, there exists a constant $c_2 > 0$ such that if the number of infected agents before a *series* of n interactions is A, where $c_2 \log n < A < n/2$, then on the conclusion of the series the number of infected agents is at least $\frac{5}{4} \cdot A$ whp $1 - n^{-\eta-1}$. Thus if we take $c_1 > c_2$ thanks to the exponential growth the number of infected agents after $O(n \log n)$ meaningful interactions is at least $n/2$ whp $1 - O(n^{-\eta-1} \log n)$. Further, by taking an extra $O(n \log n)$ pairwise interactions each uninfected (yet) agent interacts $c_3 \log n$ times, where one can choose a constant c_3, s.t., the probability of not getting infected during these interactions is at most $n^{-\eta-2}$. Finally, by the Union bound the probability of failure in one of these series of interactions is at most $n^{-\eta-1} + O(n^{-\eta-1} \log n) + n \cdot n^{-\eta-2} < n^{-\eta}$. ■

For the simplicity of presentation we assume in the next few lemmas that the agents start in phase 0. The purpose of these lemmas is to bound from above the sizes of sets of agents in phases $1, 2, 3, \ldots$ on the conclusion of $O(n \log n)$ interactions. There are separate lemmas for the ordinary and the external modes. We assume also $\varepsilon = \frac{3}{3k+2}$ and $k < m/4$.

Lemma 2 *Assume $j \leq k$ and interactions of the phase clock are performed in the ordinary mode. Assume also that at some point the number of agents in phase $x \geq_m i$ is at most $A \cdot n^{1-i\varepsilon}$, for all $i = 0, 1, \ldots, j$ and some value $A \in [1, n^{\varepsilon/3}]$. Then after $n/4$ interactions the number of agents in phase $x \geq_m i$ is at most $3A \cdot n^{1-i\varepsilon}$, for all $i = 0, 1, \ldots, j$ and whp at least $1 - 2jn^{-10}$.*

Proof: We prove this lemma by induction on j. For $j = 0$ the thesis holds since the number of agents in phase $x \geq_m 0$ is at most $n < 3A \cdot n^{1-0\cdot\varepsilon}$ with probability 1. Assume now the thesis is true for $j - 1$. By the inductive assumption after $n/4$ interactions the number of agents in phase $x \geq_m i$ is bounded from above by $3A \cdot n^{1-i\varepsilon}$, for all $i = 0, 1, \ldots, j-1$ whp $1 - 2(j-1)n^{-10}$. Two types od agents can enter phase $x \geq_m j$ during these $n/4$ interactions.

The first type refers to leaders. A leader can enter phase $x \geq_m j$ if it acts as the responder in the interaction with some initiator in phase $y \geq_m j - 1$. The number of such potential initiators is at most $3A \cdot n^{1-(j-1)\varepsilon}$ whp. And if this bound holds, during each of $n/4$ interactions ι the probability p_ι that a new leader enters phase $x \geq_m j$ in ι is at most $3A \cdot n^{1-(j-1)\varepsilon} n^{1-\varepsilon}/n^2 = 3A \cdot n^{-j\varepsilon}$. We attribute a binary 0-1 sequence σ of length $n/4$ with these interactions. Initially σ is empty and during each interaction ι we pad σ with one bit as follows. If a new leader in phase $x \geq_m j$ occurs, we add 1 to σ. If no new leader in phase $x \geq_m j$ is selected, 1 is inserted to σ

but only with probability $(3A \cdot n^{-j\varepsilon} - p_\iota)/(1-p_\iota)$ and 0 otherwise. This way all entries of σ are independently equal to 1 with probability $3An^{-j\varepsilon}$. If the number of 1s in σ is smaller or equal to $A \cdot n^{1-j\varepsilon}$, the number of new leaders in phase $x \geq_m j$ is not larger than $A \cdot n^{1-j\varepsilon}$. The expected number of 1s in σ is $\frac{3}{4}A \cdot n^{1-j\varepsilon} < n^{\varepsilon/3}$. By the Chernoff bound, the probability this number is larger than $A \cdot n^{1-j\varepsilon}$ is negligible and smaller than $e^{-n^{\varepsilon/3}/27} < n^{-10}$, for sufficiently large n. Thus the number of new leaders in phase $x \geq_m j$ is not larger than $A \cdot n^{1-j\varepsilon}$ whp $1 - n^{-10}$.

The second type of new agents in phase $x \geq_m j$ refers to followers. A follower enters phase $x \geq_m j$, if it is a responder to an initiator in phase $y \geq_m j$. Also here we attribute a 0-1 sequence ρ of length $n/4$ to the relevant interactions. Prior to these $n/4$ interactions ρ is empty. Each interaction ι extends ρ by a single bit. Let p_ι be the probability of getting a new follower in phase $x \geq_m j$ in a subsequent interaction ι. If $p_\iota > 3A \cdot n^{-j\varepsilon}$, then 1 is inserted to ρ with probability $3A \cdot n^{-j\varepsilon}$ and 0 otherwise. If $p_\iota \leq 3A \cdot n^{-j\varepsilon}$ and a new follower in phase $x \geq_m j$ occurs, 1 is added to ρ. If $p_\iota \leq 3A \cdot n^{-j\varepsilon}$ and no new follower in phase $x \geq_m j$ appears, then 1 is added to ρ with probability $(3An^{-j\varepsilon} - p_\iota)/(1-p_\iota)$ and 0 otherwise. Note that until more than $A \cdot n^{1-j\varepsilon}$ new followers appear in phase $x \geq_m j$, $p_\iota \leq 3A \cdot n^{1-j\varepsilon}/n = 3A \cdot n^{-j\varepsilon}$. If the number of 1s in ρ is smaller or equal to $A \cdot n^{1-j\varepsilon}$, the number of new followers in phase $x \geq_m j$ is not larger than $A \cdot n^{1-j\varepsilon}$. The expected number of 1s in ρ is $\frac{3}{4}A \cdot n^{1-j\varepsilon} < n^{\varepsilon/3}$. By the Chernoff bound the probability that this number is larger than $A \cdot n^{1-j\varepsilon}$ is negligible and smaller than $e^{-n^{\varepsilon/3}/27} < n^{-10}$, for sufficiently large n. Thus the number of new followers in phase $x \geq_m j$ is not larger than $A \cdot n^{1-j\varepsilon}$ whp at least $1 - n^{-10}$. This concludes the proof that the number of agents in phase $x \geq_m i$ is at most $3A \cdot n^{1-i\varepsilon}$, for all $i = 0, 1, \ldots, j$ whp at least $1 - 2jn^{-10}$. ■

We prove now the analogous lemma for the external mode.

Lemma 3 *Assume that the interactions of the phase clock are performed in the external mode. Assume also that for some integer t and a value $A \in [1, n^{\varepsilon/3}]$ just after interaction $t \cdot n/8$ of the phase clock, the number of agents in phase $x \geq_m i$ is at most $A \cdot n^{1-i\varepsilon}$, for all $i = 0, 1, \ldots, k$. Then after the next $n/8$ interactions the number of agents in phase $x \geq_m i$ is at most $3A \cdot n^{1-i\varepsilon}$, for all $i = 0, 1, \ldots, k$, and whp at least $1 - 20k \cdot n^{-10}$.*

Proof: We assume that after $t \cdot n/8$ interactions of the phase clock the number of agents in phase $x \geq_m i$ is at most $A \cdot n^{1-i\varepsilon}$, for all $i = 0, 1, \ldots, k$. Let us perform a series of $n/4$ interactions of the ordinary mode instead of $n/8$ interactions of the external mode. By Lemma 2 applied with $j = k$ after $n/4$ interactions of the ordinary mode, the probability of having $i \in \{0, 1, \ldots, k\}$, s.t., the number of agents in phase $x \geq_m i$ exceeds $A \cdot n^{1-i\varepsilon}$ is negligible and smaller than $2kn^{-10}$.

The probability that a particular agent does not act as a responder in any of these $n/4$ interactions is $(1-1/n)^{n/4} < e^{-1/4}$. Thus the expected number of agents that are not responders in these interactions is smaller than $ne^{-1/4}$. The probability that the number of these responders is smaller than $n/8$ is the same as the probability that the number of agents not being responders is larger than $\frac{7}{8}n$. By the Markov inequality this probability is at least $1 - \frac{ne^{-1/4}}{7n/8} > 1/10$.

Let event B happen when there are at least $n/8$ responders during these (ordinary mode) interactions. We just proved that $\Pr(B) > 1/10$. Let event C occur when after $n/4$ interactions of the ordinary mode there exists $i \in \{0, 1, \ldots, k\}$, s.t., the number of agents in phase $x \geq_m i$ exceeds $A \cdot n^{1-i\varepsilon}$. Let event D occur when after $n/8$ interactions of the external mode there exists $i \in \{0, 1, \ldots, k\}$ such that the number of agents in phase $x \geq_m i$ exceeds $A \cdot n^{1-i\varepsilon}$. We have $\Pr(D) < \Pr(C|B)$, since from $n/4$ interactions of the ordinary mode one can choose the first $n/8$ interactions with different responders. During the $n/8$ interactions propagation of agents in each phase $x \geq_m i$ is weaker comparing to all $n/4$ interactions. By the Bayes rule we get

$$\frac{1}{10} \cdot \Pr(D) < \Pr(B)\Pr(C|B) + \Pr(\bar{B})\Pr(C|\bar{B}) \leq 2kn^{-10}.$$

Thus we can conclude $\Pr(D) < 20kn^{-10}$. ■

The following lemmas apply to both the ordinary and external modes of the phase clock.

Lemma 4 *Assume all agents start in the clock phase 0. The probability that after* $\frac{1}{8(3k+2)} n \log n$ *interactions (in either of the phase clock modes) there are at least* $n^{2/(3k+2)}$ *agents in phase* $x \geq_m k$ *is at most* $20(\varepsilon/3)k \log n \cdot n^{-10}$.

Proof: In the beginning the number of agents in phase $x \geq_m i$ is at most $3A \cdot n^{1-i\varepsilon}$, for all $i = 0, 1, \ldots, k$ and $A = 1$. To conclude the proof we apply Lemma 2 (or Lemma 3, respectively to the mode) $\frac{1}{3k+2} \log n$ times for the series of $\frac{1}{8(3k+2)} n \log n$ subsequent interactions. ■

Lemma 5 *Assume all agents start in the clock phase 0. The probability that on the conclusion of* $\frac{n \log n}{8(3k+2)}$ *interactions (in either of the phase clock modes) there are some agents in clock phase* $x \geq_m k+1$ *is* $O(n^{-\varepsilon/3} \log n)$.

Proof: The clock phase $x = k+1$ can be entered only by a leader which acts as the responder in the interaction with an agent in a clock phase $x = k$. Since the number of agents in clock phase $x = k$ is at most $n^{2\varepsilon/3}$, the probability of having such interaction is at most $n^{1-\varepsilon/3}$. By the Union bound the probability of having such interaction during $\frac{n \log n}{8(3k+2)}$ subsequent interactions is $O(n^{-\varepsilon/3} \log n)$. ■

Lemma 6 *Assume all agents start in the clock phase* $x = 0$ *and* d *is a positive constant. Then there exists an integer constant* $K < m/2$, *such that the first agent enters phase* $x = K$ *before interaction* $t + dn \log n$ *with negligible probability at most* $n^{-\eta}$, *for sufficiently large* n .

Proof: Assume $K = \kappa k$. We can divide all phases $x = 1, 2, \ldots K$ into κ consecutive chunks having k phases each. Let t_i, for all $i = 0, 1, 2, \ldots, \kappa - 1$, be the first interaction in which an agent enters phase $i \cdot k + 1$, where $t_0 = 0$. By Lemma 5 the probability that $t_i - t_{i-1} < \frac{n \log n}{8(3k+2)}$ is smaller than $cn^{-\varepsilon/3} \log n$, for some constant $c > 0$. The probability, that for κ' different values i we have $t_i - t_{i-1} \leq \frac{n \log n}{8(3k+2)}$ is by the binomial distribution smaller than

$$n \binom{\kappa}{\kappa'} \left(cn^{-\varepsilon/3} \log n \right)^{\kappa'}.$$

Now take $\kappa' > 3\eta/\varepsilon$ and $\kappa - \kappa' > d8(3k+2)$. For sufficiently large n we obtain $t_\kappa \leq dn \log n$ with probability at most $n^{-\eta}$. ■

Lemma 7 *For any constant* d *there is another constant* K, *s.t., if* $K < m/4$ *and after interaction* t *there is an agent in phase* i *and all other agents are in phases* $x : i - K \leq_m x \leq_m i$, *then whp*

- *the first interaction* t' *when an agent enters phase* $i + K$ *satisfies* $t' > t + dn \log n$, *and*
- *during interaction* t' *all agents are in phases* x, *such that* $i \leq_m x \leq_m i + K$.

Proof: By Theorem 1 and Lemma 1 there exists a positive constant d', s.t., one way epidemic succeeds within $d' \cdot n \log n$ interactions whp. By Lemma 6 for a constant $D = \max\{d, d'\}$ there is K, s.t., all agents starting in phase i move to phase at most $i + K$ after $Dn \log n$ interactions whp. Thus $t' > Dn \log n \geq dn \log n$ whp. Since one way epidemic initiated by an agent in phase i during interaction t succeeds whp, all agents after interaction t' are in phase $x \geq_m i$ whp. ■

Consider now the interactions in which phase clocks in different agents pass through 0. We say that passes through 0 of two agents are *equivalent* if they occur during a period in which all agents are in phases $x : 3m/4 <_m x <_m m/4$. This notion defines an equivalence relation which is reflexive, symmetric and transitive, and in turn passes of agents through 0 form *equivalence classes*. This allow us to use argumentation similar to the one proposed in [4], however this time for the junta of leaders rather than for a single leader.

Theorem 2 *Assume all agents start the phase clock protocol from the initial phase* 0 *when* $n^{1-\varepsilon}$ *leaders and* $n - n^{1-\varepsilon}$ *followers are already selected. For any fixed* $\varepsilon, \eta, d_1, d_2 > 0$*, there exists a constant* m*, such that, the finite-state phase clock with parameter* m *completes* n^η *passes through* 0*, s.t., the following conditions are satisfied with high probability* $1 - n^{-\eta}$*, for sufficiently large* n*.*

- *The passes through* 0 *form equivalence classes for all agents and the number of interactions between closest passes through* 0 *in different equivalence classes is at least* $d_1 n \log n$*.*
- *The number of interactions between two subsequent passes through* 0 *in any agent is smaller than* $d_2 n \log n$ *whp.*

Proof: If $d = d_1$, by Lemma 7 there exists K, s.t., or $m = 5K$ the thesis of this Lemma holds. We consider five subsets A_0, A_1, A_2, A_3, A_4 of $\mathbb{Z}_{5K}$ defined as $A_i = \{iK, iK + 1, \ldots, iK +_m K\}$. By Lemma 7 phases of all agents progress whp from A_i to $A_{i+_5 1}$ (modulo 5) in at least $d_1 n \log n$ interactions whp. This implies that agents' passes through 0 form equivalence classes whp and the number of interactions between closest passes through 0 in different equivalence classes is at least $d_1 n \log n$ whp. Since one way epidemic is done in $O(n \log n)$ interactions whp each agent increments its phase in $O(n \log n)$ interactions. Thus the number of interactions between two subsequent passes through 0 in any agent is smaller than $d_2 n \log n$ whp. ■

As indicated, we run the phase clock in the ordinary and the external modes simultaneously. This is to run two time loops: the *external*, controlled by the external mode, and the *internal*, controlled by the ordinary mode. In the leader election protocol we will use $\Theta(\log n)$ *iterations* of the *external loop* coresponding to $\Theta(\log n)$ executions of multi-broadcast to the whole population. Each execution is implemented via $\Theta(n \log n)$ interactions controlled by the ordinary mode of the phase clock. A meaningful interaction in the external mode happens after an agent whose ordinary clock passes or just passed through 0 interacts for the first time as the responder with an agent with phase in $\{0, 1, 2, \ldots, \lceil m/2 \rceil\}$. These passes through 0 form further equivalence classes of agents.

Now consider set A_0 from the proof of Theorem 2 for the ordinary mode (internal loop). An agent starting in phase in A_5 at some point interacts for the first time with an agent with clock in phase in A_0. After this interaction the follower moves to phase $x \geq_m 0$, and the leader moves to phase $x \geq_m 1$. The order in which agents are picked for these interactions is random. Once an agent experiences such interaction, its next interaction as the responder will be *meaningful* for phase clock operation in the external mode. This way phase clock in the external mode can associate $\Theta(\log n)$ iterations of the internal loop of the phase clock run in the ordinary mode.

In conclusion, we formulate two useful facts related to phase clocks. Fact 1 states that if some leaders become followers during the phase clock protocol, then the phase clock can only slow down, but the upper bound on the number of interactions remains $O(n \log n)$. Fact 2 states that any unsuccessful interactions can only slow down the phase clock.

Fact 1 *The reduction of the number of leaders during the execution of the phase clock protocol can only slow down phase progression of agents on their clocks. And if at least one agent remains the leader the number of interactions between two subsequent passes through* 0 *in any agent is still bounded by* $O(n \log n)$ *whp.*

Fact 2 *If some interactions of the phase clock are faulty, i.e., they do not result in progression, then the phases of all agents do not become larger comparing to the protocol without faults.*

4 Forming a junta

In this section we describe a protocol `Forming_junta` which purpose is to elect from n identical agents a junta of $O((n \log n)^{1/2})$ leaders assuming $O(\log \log n)$ states at each agent. This junta of leaders will be used to support phase clocks and eventually selection of a unique leader.

The states of agents are represented as pairs (l, a) where $a \in \{0, 1\}$. The value l is a non-negative integer which we refer to as *level*. During execution of the protocol agents with $a = 0$ do not update their states. However, any agent v with value $a = 1$ increments its level l by 1 or changes its value a to 0 during all interactions v participates in. The protocol stabilizes when all agents conclude with $a = 0$. The transition function is defined, s.t., on the conclusion of this protocol there are $O((n \log n)^{1/2})$ agents holding the highest computed value l whp. These agents form the desired *junta of leaders*.

In the beginning all agents start in the same state $(l, a) = (0, 1)$. As agents in states $(l, 0)$ do not get updated, we only need to specify how agents in states $(l, 1)$ are changed during pairwise interactions. The transition function at level $l = 0$ differs from $l > 0$. If an agent in state $(0, 1)$ interacts with another agent in state $(0, 1)$, the final state of the initiator is $(1, 1)$ and $(0, 0)$ of the responder

$$(0, 1), (0, 1) \to (0, 0), (1, 1).$$

If an agent v in state $(0, 1)$ interacts with any agent in state (l, a), for levels $l > 0$, or with an agent in state $(0, 0)$, then the resulting state of v is $(0, 0)$. If an agent v in state $(l, 1)$ for $l > 0$ interacts, its state changes only if v acts as the responder. If the initiator is in state (l', a) such that $l \leq l'$, then the responder's state becomes $(l + 1, 1)$. If the initiator is in state (l', a), such that $l > l'$, then the responder's state becomes $(l, 0)$.

Denote by B_l the number of agents which reach level l during execution of the protocol `Forming_junta`. The actual value of B_l depends on the particular execution thread of the protocol. We first prove an upper bound on B_1.

Lemma 8 *For n large enough $1 \leq B_1 \leq n/2$.*

Proof: During an interaction between two agents in states $(0, 1)$ exactly half of the participating agents increase their level l to 1. The remaining half ends up in state $(0, 0)$ which becomes their final state. During any other interaction in which an agent v in state $(0, 1)$ participates, v changes its state to $(0, 0)$. So at least half of the agents end up in state $(0, 0)$. Finally, since the first interaction of the protocol is between two agents in states $(0, 1)$, so at least one agent results in a state with $l > 0$. ■

Due to the reduction property of the protocol we have $B_1 \geq B_2 \geq B_3 \geq B_4 \geq \ldots$. And in particular there exists the last L for which value $B_L > 0$. As our aim is to prove $L = O(\log \log n)$ and in turn $B_L = O(\sqrt{n \log n})$, we get there by limiting values of B_l, for all $l > 1$.

Lemma 9 *Assume $n^{-1/3} \leq A < 1$ and $B_l \leq A \cdot n$, then $B_{l+1} \leq \frac{11}{10} A^2 \cdot n$ whp $1 - e^{-n/300}$.*

Proof: An agent v contributing to value B_l results in state $(l, 1)$ as soon as it gets to level l during the relevant interaction t. Consider the first interaction ι succeeding t in which v acts as the responder. With probability $p_\iota \leq B_l/n \leq A$ during this interaction the initiator is on level $l' \geq l$. Thus v moves to level $l + 1$ with probability at most A as otherwise the responder would end up in state $(l, 0)$ and would not contribute to B_{l+1}. Consider now the sequence of all B_l interactions ι, in which agents in state $(l, 1)$ act as responders. We can attribute to this sequence a binary 0-1 sequence σ of length B_l, s.t., if during interaction ι an agent ends up in state $(l + 1, 1)$, the respective entry in σ becomes 1. Otherwise, this entry becomes 1 with probability $(1-A)/(1-p_\iota)$ and 0 with probability $A/(1-p_\iota)$. Thus the probability of each entry being 1 is independently equal to A and the number of 1s in σ is at least B_{l+1}. The expected number of these 1s is $A \cdot B_l \leq A^2 n$. By the Chernoff bound $B_{l+1} > \frac{11}{10} A^2 \cdot n$ with probability at most $e^{-A^2 n/300}$. ■

Lemma 10 *If $B_l \leq n^{1/3}$ we get $B_{l+1} > 0$ with probability at most $n^{-1/3}$.*

Proof: If $B_l \leq n^{1/3}$, the probability for any agent on level l to get to level l is at most $n^{-2/3}$. Thus by the Union bound the probability of some agent getting to level l is at most $n^{-1/3}$. ■

Lemma 11 *There exists a positive constant c, s.t., if $B_l \geq c\sqrt{n \log n}$ then the probability of $B_{l+1} = 0$ is negligible.*

Proof: Consider a group of $c\sqrt{n \log n}/2$ agents which move to level l after this level is already reached by $c\sqrt{n \log n}/2$ other agents. Any agent in this group moves to level $l+1$ with probability at least $c\sqrt{\log n/4n}$. Since all these agents advance to level $l+1$ independently, the probability that $B_{l+1} = 0$ is at most

$$\left(1 - c\sqrt{\log n/4n}\right)^{c\sqrt{n \log n}/2} < e^{-c^2 \log n/4} < n^{-c^2/4}$$

This last value is smaller than $n^{-\eta}$, for c large enough. ■

Theorem 3 *In protocol* `Forming_junta` *the largest level L for which $B_L > 0$ satisfies $L = O(\log \log n)$ and $B_L = (\sqrt{n \log n})$ whp.*

Proof: By Lemma 8 we have $B_1 \leq n/2$. By Lemma 9 we conclude $B_2 \leq \frac{11}{10} \cdot \frac{n}{4}$ whp $e^{-n/300}$. Furthermore $B_3 \leq (\frac{11}{10})^3 \cdot \frac{n}{2^4}$ whp $2e^{-n/300}$. And in general $B_l \leq (\frac{11}{10})^{2^l-1} \cdot n2^l$ whp $le^{-n/300}$. Thus for some $L' = O(\log \log n)$ we get $B_{L'} \leq n^{1/3}$, an by Lemma 10 the value B'_L, where L'=L+c, equals 0 for some constant c whp $1 - n^{-\eta-1}$. By Lemma 11 on the last level L for which $B_L > 0$ we have $B_L = (\sqrt{n \log n})$ whp $1-n^{-\eta-1}$. Thus both conditions hold whp $1-n^{-\eta}$. ■

The last lemma bounds from above the running time of protocol `Forming_junta`.

Lemma 12 *The protocol* `Forming_junta` *stabilizes in $O(n \log n)$ iteractions whp.*

Proof: Recall from Lemma 8 that $B_1 \leq n/2$ and the number of agents with the final state $(0, 0)$ is at least $n/2$. Each agent in this group ends up in this state during its first interaction. Since every agent interacts at least once during the first $O(n \log n)$ interactions of the protocol whp, all agents ending up in state $(0, 0)$ they do so during this time. One can show that an agent does not experience an interaction during the first $cn \ln n$ interactions with probability

$$\left(1 - \frac{2}{n}\right)^{cn \ln n} \leq n^{-2c}.$$

Thus there exists a positive constant c for which after $cn \ln n$ interactions each agent experiences its first interaction whp $1 - n^{-\eta-1}$. Any agent that interacts as the responder with an agent in state $(0, 0)$ sets its value a to 0 which concludes the transition process. After at least $n/2$ agents are in state $(0, 0)$, the probability that the current interaction is one of such interactions w.r.t. a particular responder is at least $\frac{1}{4n}$. Thus the probability that a given agent does not have $a = 0$ after $c'n \ln n$ iterations is

$$\left(1 - \frac{1}{4n}\right)^{c'n \ln n} \leq n^{-c'/4}.$$

And for c' big enough $n^{-c'/4} < -\eta - 1$. Thus the number of interactions needed to obtain $a = 0$ in all agents is $O(n \log n)$ whp. ■

Finally we prove a Corollary stating that "spoiling" (for the definition check below) protocol `Forming_junta` does not affect validity of statements of Theorem 3 and Lemma12. Using the notion of a spoiled protocol instead of the flawless one is needed to bound the total number of states in the leader election protocol to $O(\log\log n)$. Let *spoiled* `Forming_junta` protocol be any protocol obtained by changing some states spontaneously from (l, a) to $(0, 0)$, where l is not the highest level reached so far in the population. We denote the total numbers of agents that reach level l in this spoiled protocol by B_l^*. And we denote the highest level for which $B_l^* > 0$ by L^*. Observe that in the spoiled protocol all agents at level L^* never go through state $(0, 0)$.

Corollary 1 *Level L^* satisfies the condition $L^* = O(\log\log n)$ and $B_{L^*}^* = O(\sqrt{n\log n})$ whp. Also spoiled* `Forming_junta` *protocol stabilizes after $O(n\log n)$ interactions whp.*

Proof: The numbers of agents B_l^* reaching level l in the spoiled protocol are not larger respectively than numbers B_l from the flawless protocol, thus $L^* = O(\log\log n)$. Also Lemma 11 still bounds from above $B_{L^*}^*$ by $O(\sqrt{n\log n})$ whp. Thus the running time of the spoiled protocol is not larger than the flawless one. ■

5 Leader election

In this section we describe how to combine protocols described in the two previous sections to derive a fast population protocol for leader election. This new leader election protocol operates in time $O(\log^2 n)$ on populations with agents equipped with $\Theta(\log\log n)$ states.

The new leader election protocol assumes that at the beginning there is a non-empty subset (possibly the whole population) of agents which are candidates for leaders, and this subset is gradually reduced to a singleton. The protocol consists of $\Theta(\log n)$ iterations of the external loop, each formed of $\Theta(n\log n)$ interactions controlled by the ordinary mode of the phase clock. During each iteration every candidate picks independently at random a bit 0 or 1 by tossing a fair coin. In real terms, the coin tossing process relies on the initiator vs responder selection performed by the random scheduler. The candidates which pick 1 broadcast message "1" to all other agents. And when a candidate with chosen 0 receives message "1" it stops being a candidate for the leader.

Theorem 4 *The protocol proposed above selects a unique leader during $\Theta(\log n)$ iterations whp.*

Proof: If the number of candidates is at least 2, the probability that in the relevant iteration at least half of the candidates draw 0 is at least 1/2. Consider a series of $c\log n$ consecutive iterations and form a binary 0-1 sequence σ of length $c\log n$, in which the entries correspond to these iterations. If prior to an iteration only one candidate remains, the entry in σ is chosen uniformly at random by a single coin toss. If there are more candidates and more draw 1s than 0s, then the relevant entry becomes 1. If there is more than one candidate and at least half of them draw 0, en extra random selection is triggered, s.t., the probability of choosing 0 is exactly 1/2. Note, that if the sequence has at least $\log n$ 1s, then exactly one leader remains. By the Chernoff bound the probability, that σ contains less than $\log n$ 1s is smaller than $e^{-(1-1/c)^2 c\log n/2}$, and in turn smaller than $n^{-\eta}$, for a constant c large enough. ■

The main problem with utilisation of the protocol described above is the need of implementing a counter of $\Theta(\log n)$ iterations with the help of a small memory. We also need to implement multi-broadcast of 1s which takes $\Theta(n\log n)$ interactions whp. The multi-broadcast can be implemented via one way epidemic described in section 2. The two processes can be controlled by the phase clock run in both the external and the ordinary modes respectively, using a constant number of states. This is conditioned by forming a junta of at most $n^{1-\varepsilon}$ leaders. In section 4

we described the relevant `Forming_junta` protocol which reduces the number of leaders to $O(\sqrt{n \log n})$ and operates on $\Theta(\log \log n)$ states at each agent. Our leader election protocol starts with a single execution of protocol `Forming_junta` which is followed by application of the leader reduction mechanism in order to reduce the size of junta to a single leader.

Each agent enters the leader election protocol in the same state, where the current state of an agent is represented by a vector (l, a, b, x, y, z). A non-negative integer l refers to the number of levels bounded by $O(\log \log n)$. Other positions contain small integer constants $a \in \{0, 1\}$, $b \in \{\texttt{leader}, \texttt{follower}\}$, which refer to the leadership status, and $x, y \in \mathbb{Z}_m$ are utlised for the phase clock's ordinary and external modes respectively. The remaining state overheads imposed by our protocol are encoded in z which is limited to a constant number of values, and will not be discussed explicitly here. Thus the number of states utilised by our protocol is $O(\log \log n)$.

Each agent starts the leader election protocol in state $(l, a, b, x, y) = (0, 1, \texttt{leader}, 0, 0)$. It runs the protocol `Forming_junta` in state (l, a), for as long as $b = \texttt{leader}$. As soon as b gets value `follower`, which is irreversible, the state of this agent for the purpose of protocol `Forming_junta` becomes $(0, 0)$. This happens only when l is not at the highest level in the population, so the protocol `Forming_junta` gets occasionally spoiled this way. Once value a becomes 0, the agent starts its phase clock on level l as the leader with parameters $x = y = 0$. If an agent at level l interacts with an agent with the phase clocks on a higher level $l' > l$, then its state is rewritten $(l, a, b, x, y) \leftarrow (l', 0, \texttt{follower}, 0, 0)$. This way the agent aligns its phase clocks in phase 0 on level l' and ends up in state $(0, 0)$ in the spoiled protocol `Forming_junta`. The level of the phase clock can be incremented this way many times until it attains the maximum level L^* ever reached by the population. Thus in the end all agents together run the phase clock on level L. Agents that advance to level L^* in spoiled `Forming_junta` protocol are the leaders of the phase clocks and other agents are the followers.

We run the phase clock in the ordinary mode and in the external mode simultaneously to implement the two loops described on page 8 (below Theorem 2). The phase clock in the ordinary mode is driven by all interactions in which the responder has value $a = 0$. If the responder interacts with an initiator on a higher level it advances its clock level as described in the previous paragraph. If the responder has the same clock level as the initiator, they both perform one interaction in the ordinary mode. If the responder interacts with the initiator on a lower level or having $a = 1$, then this interaction is void in the ordinary mode. The phase clock operates in the ordinary mode until it passes through 0 for the first time. And it counts for each agent the first $\Theta(n \log n)$ iteractions by Fact 2.

According to Corollary 1 each agent should conclude spoiled `Forming_junta` protocol in the first $\Theta(n \log n)$ interactions whp. Then each remaining leader v chooses randomly 0 or 1 during the first interaction with a non-leader after the phase (in the ordinary mode of the clock) v is in passed through 0. If the non-leader is the initiator, v chooses 1 otherwise v chooses 0. This gives a truly random value to each leader, and since there are $O(\sqrt{n \log n})$ leaders this process is completed whp during a constant number of interactions. After choosing 0 or 1 at random, leaders multi-broadcast 1s to the whole population via one-way epidemic. The $\Theta(n \log n)$ interactions required by multi-broadcast are counted with the help of the phase clock in the ordinary mode. In order to obtain a unique leader whp, this process is iterated $\Theta(\log n)$ times by the external loop and controlled by the phase clock in the external mode. The protocol concludes at each agent, when its external clock attains phase $m - 1$. The following theorem holds.

Theorem 5 *The protocol described above finds a unique leader in $O(n \log^2 n)$ interactions whp.*

Now we formulate a Las Vegas type variant of our algorithm to match the existing lower bound $\Omega(\log \log n)$ on the number of states in fast leader election [6].

Theorem 6 *For agents equipped with $O(\log \log n)$ states, there exists a leader election protocol which always gives the correct answer and works in parallel time $O(\log^2 n)$ whp.*

Proof: In the Las Vegas type protocol the external clock utilises the set of transitions defined as before, however, we can replace $\max_m$ by the standard maximum as we assume that the clock stops after reaching phase $m-1$. We also allow an agent v to utilise in its external clock all subsequent interactions as meaningful after v in a very unlikely event interacts with any other agent with *a distant* ordinary phase clock value. This happens when the relevant phase clock values x and $x +_m a$ satisfy $m/5 < a < 4m/5$. In addition, after an agent starts using all interactions as meaningful (in the external clock), it also infects with this setting all other agents it interacts with subsequently. By Theorem 5 we can construct a fast leader election protocol with the clock phases drawn from $\mathbb{Z}_m$, s.t., a single leader is elected and the external phase clocks in all agents conclude in phase $m-1$ during the first $O(n \log^2 n)$ interactions whp $1 - n^{-10}$. Thanks to Lemma 7 used in the proof of correctness of the relevant clock construction we can derive an extra observation that no two agents can have distant ordinary phase clock values during execution of the protocol whp $1 - n^{-10}$.

If a leader enters phase $m-1$ in the fast protocol we have just described, it can no longer be eliminated by this protocol. Independently, all agents run from the beginning a slow two-state leader election protocol which works with the expected number of interactions $O(n^2 \log n)$ [24]. In this slow protocol, whenever two leader candidates interact directly, the initiator eliminates the responder. If a leader candidate of this slow protocol reaches phase $m-1$ in the external clock, it stops being a candidate for the leader, unless it is still a leader in the fast protocol. Leaders reaching phase $m-1$ in the external clock eliminate other leaders in the fast protocol in direct pairwise interactions according to the slow protocol principle.

Note that all agents complete `Forming_junta` protocol in the expected number of $O(n \log n)$ interactions. Assume this part of leader election is already completed. Let E be the expected number of interactions in the leader election algorithm. We have

$$E \leq (1 - n^{-10}) \cdot cn \log^2 n + n^{-10} \max\{E', E''\}$$

In this formula E' and E'' are the expected numbers of interactions if we start from the worst case configurations respectively not containing (E') and containing (E'') distant ordinary clock phases. If we start from the configuration not containing distant ordinary clock phases, the external phase clock reaches phase $m-1$ in all agents or all leaders disappear in $O(n \log^2 n)$ interactions whp $1 - n^{-10}$, unless an interaction between agents with distant ordinary clock phases occurs at some point. This can be proved using Lemma 6 using the argument analogous to the proof of Lemma 7. In the latter case the external clock reaches phase $m-1$ whp in $O(n \log n)$ interactions (after this distant interaction takes place) unless all leaders in the fast protocol disappear. When the fast leader election protocol fails, i.e., it either produces multiple leaders or all candidates for leaders disappear, the leader election process is completed during $O(n^2 \log n)$ interactions of the slow leader election protocol.

$$E' \leq (1 - n^{-10}) \cdot cn^2 \log n + n^{-10} \max\{E', E''\}$$

If $E' \geq E''$ we get $E', E'' = O(n^2 \log n)$ from this inequality. When we start in the worst case configuration in which there are two agents with distant ordinary phase clock values, they meet in the first interaction of the protocol with probability at least n^{-2}. And when this happens, the external clock reaches phase $m-1$ in $O(n \log n)$ interactions whp and also in this case the unique leader is selected whp during $O(n^2 \log n)$ interactions of the slow protocol. Thus

$$E'' \leq n^{-2} \cdot cn^2 \log n + (1 - n^{-2})(\max\{E', E''\} + 1)$$

If $E'' \geq E'$, we get $E', E'' = O(n^2 \log n)$ from this inequality. And since $E', E'' = O(n^2 \log n)$ we conclude $E = O(n \log^2 n)$. ■

6 Conclusion

We studied in this paper fast and space efficient leader election in population protocols. Our new protocol stabilises in (parallel) time $O(\log^2 n)$ when each agent is equipped with $O(\log \log n)$ states. This double logaritmic space utilisation matches asymptotically the lower bound $\frac{1}{2} \log \log n$ on the minimal number of states required by agents in any leader election algorithm with the running time $o(\frac{n}{\text{polylog } n})$, see [6]. For the convenience of the reader we provide below the logical structure of the full argument in the form of a diagram, see Figure 1.

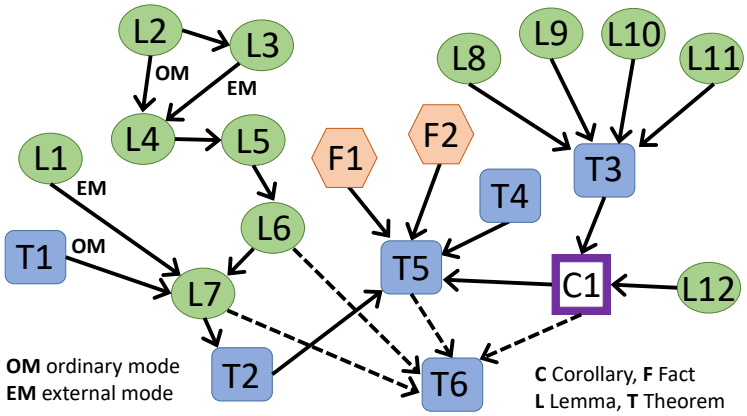

Figure 1: The structure of the argument

There are several interesting unanswered questions left for further consideration. For example, whether one can select whp a unique leader in time $o(\log^2 n)$ with $O(\log \log n)$ states available at each agent. Another interesting direction is the design of a fast $O(\log \log n)$-space majority population protocol, which would provide a natural complement to the results in [6] and this paper. Also, the exact space complexity of majority as well as plurality consensus in deterministic population protocols considered recently, e.g., in [30] still require better understanding.

References

[1] D. Angluin, Local and global properties in networks of processors, Proc. *12th Annual ACM Symposium on Theory of Computing*, STOC 1980, 82–93.

[2] D. Angluin, J. Aspnes, Z. Diamadi, M.J. Fischer, and R. Peralta, Computation in networks of passively mobile finite-state sensors. Proc. *23rd Annual ACM Symposium on Principles of Distributed Computing*, PODC 2004, 290–299.

[3] D. Angluin, J. Aspnes, Z. Diamadi, M.J. Fischer, and R. Peralta, Computation in networks of passively mobile finite-state sensors. Distributed Computing, 18(4), 2006, 235–253.

[4] D. Angluin, J. Aspnes, D. Eisenstat. Fast computation by population protocols with a leader, Distributed Computing 21(3), 2008, 183–199.

[5] D. Angluin, J. Aspnes, and D. Eisenstat. A simple population protocol for fast robust approximate majority, Distributed Computing, 21(2), 2008, 87–102.

[6] D. Alistarh, J. Aspnes, D. Eisenstat, R. Gelashvili and R.L. Rivest, Time-Space Trade-offs in Population Protocols, Proc. *28th Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA 2017, 2560–2579.

[7] D. Alistarh and R. Gelashvili, Polylogarithmic-time leader election in population protocols, Proc. *42nd International Colloquium on Automata, Languages, and Programming*, ICALP 2015, 479–491.

[8] A. Arora, S. Dolev, and M.G. Gouda, Maintaining digital clocks in step, Proc. *5th International Workshop on Distributed Algorithms*, (LNCS 579) 1991, 71–79.

[9] H. Attiya and M. Snir, Better Computing on the Anonymous Ring, Journal of Algorithms 12, 1991, 204–238.

[10] H. Attiya, M. Snir, and M. Warmuth, Computing on an Anonymous Ring, Journal of the ACM 35, 1988, 845–875.

[11] H. Attiya and J. Welch, Distributed Computing: Fundamentals, Simulations, and Advanced Topics, 2nd Edition, Willey, April 2004.

[12] L. Becchetti, A.E.F. Clementi, E. Natale, F. Pasquale, and R. Silvestri, Plurality consensus in the gossip model, Proc. *26th Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA 2015,371–390.

[13] P. Berenbrink, T. Friedetzky, G. Giakkoupis, and P. Kling. Efficient plurality consensus, or: The benefits of cleaning up from time to time. Proc. *43rd International Colloquium on Automata, Languages, and Programming*, ICALP 2016, 1–14.

[14] P. Boldi, S. Shammah, S. Vigna, B. Codenotti, P. Gemmell, and J. Simon, Symmetry Breaking in Anonymous Networks: Characterizations, Proc. *4th Israel Symposium on Theory of Computing and Systems*, ISTCS 1996, 16–26.

[15] P. Boldi and S. Vigna, Computing Anonymously with Arbitrary Knowledge, Proc. *18th ACM Symp. on Principles of Distributed Computing*, PODC 1999, 181–188.

[16] J.E. Burns, A Formal Model for Message Passing Systems, Tech. Report TR-91, Computer Science Department, Indiana University, Bloomington, September 1980.

[17] I. Chatzigiannakis, O. Michail, S. Nikolaou, A. Pavlogiannis, and P.G. Spirakis, Passively mobile communicating machines that use restricted space. Proc. *7th ACM ACM SIGACT/SIGMOBILE International Workshop on Foundations of Mobile Computing*, 2011, 6–15.

[18] H.-L. Chen, R. Cummings, D. Doty, and D. Soloveichik, Speed faults in computation by chemical reaction networks, Distributed Computing, Springer 2014, 16–30.

[19] D. Dereniowski and A. Pelc, Leader election for anonymous asynchronous agents in arbitrary networks, Distributed Computing 27, 2014, 21–38.

[20] S. Dobrev and A. Pelc, Leader Election in Rings with Nonunique Labels, Fundamenta Informaticae 59, 2004, 333–347.

[21] S. Dolev and J.L. Welch, Self-stabilizing clock synchronization in the presence of Byzantine faults, Journal of the ACM, 51(5), 2004, 780–799.

[22] D. Doty, Timing in chemical reaction networks. Proc. *25th Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA 2014, 772–784. SIAM.

[23] A. Daliot, D. Dolev, and H. Parnas, Self-stabilizing pulse synchronization inspired by biological pacemaker networks, Proc. *Self-Stabilizing Systems*, SSS 2003, 32–48.

[24] D. Doty and D. Soloveichik, Stable leader election in population protocols requires linear time, Proc. *29th International Symposium on Distributed Computing*, DISC 2015, 602–616.

[25] P. Flocchini, E. Kranakis, D. Krizanc, F.L. Luccio and N. Santoro, Sorting and Election in Anonymous Asynchronous Rings, Journal of Parallel and Distributed Computing 64, 2004, 254–265.

[26] G.N. Fredrickson and N.A. Lynch, Electing a Leader in a Synchronous Ring, Journal of the ACM 34, 1987, 98–115.

[27] E. Fusco and A. Pelc, Knowledge, level of symmetry, and time of leader election, Proc. *20th Annual European Symposium on Algorithms*, ESA 2012, 479–490.

[28] E. Fusco, A. Pelc, Trade-offs between the size of advice and broadcasting time in trees, Algorithmica 60, 2011, 719–734.

[29] L. Gąsieniec, D.D. Hamilton, R. Martin, and P.G. Spirakis, The match-maker: Constant space distributed majority via random walks, Proc. *17th International Symposium on Stabilization, Safety, and Security of Distributed Systems*, SSS 2015, 67–80.

[30] L. Gąsieniec, D. Hamilton, R. Martin1, P.G. Spirakis and G. Stachowiak, Deterministic Population Protocols for Exact Majority and Plurality, OPODIS'16 (post-conference proceedings, to appear).

[31] M. Ghaffari and M. Parter, A polylogarithmic gossip algorithm for plurality consensus. Proc. *34th Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing*, PODC 2016, 117–126.

[32] Ch. Glacet, A. Miller, and A. Pelc, Time vs. Information Tradeoffs for Leader Election in Anonymous Trees, Proc. *27th annual ACM-SIAM symposium on Discrete algorithms*, SODA 2016, 600–609

[33] M.A. Haddar, A.H. Kacem, Y. Métivier, M. Mosbah, and M. Jmaiel, Electing a Leader in the Local Computation Model using Mobile Agents, Proc. *6th ACS/IEEE International Conference on Computer Systems and Applications*, AICCSA 2008, 473–480.

[34] T. Herman, Phase clocks for transient fault repairs, IEEE Transactions on Parallel and Distributed Systems 11(10), 2000, 1048–1057.

[35] D.S. Hirschberg, and J.B. Sinclair, Decentralized Extrema-Finding in Circular Configurations of Processes, Communications of the ACM 23, 1980, 627–628.

[36] G. Le Lann, Distributed Systems - Towards a Formal Approach, Proc. *IFIP Congress*, 1977, 155–160.

[37] Y. Mocquard, E. Anceaume, J. Aspnes, Y. Busnel, and B. Sericola, Counting with population protocols, Proc. 2015 *IEEE 14th International Symposium on Network Computing and Applications*, NCA 2015, 35–42.

[38] G.B. Mertzios, S.E. Nikoletseas, C. Raptopoulos, and P.G. Spirakis, Determining majority in networks with local interactions and very small local memory. Proc. *41st International Colloquium on Automata, Languages, and Programming*, ICALP 2014, 871–882.

[39] O. Michail and P.G. Spirakis, Simple and efficient local codes for distributed stable network construction, Proc. *32nd Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing*, PODC 2014, 76–85.

[40] G.L. Peterson, An $O(nlogn)$ Unidirectional Distributed Algorithm for the Circular Extrema Problem, ACM Transactions on Programming Languages and Systems 4, 1982, 758–762.

[41] M. Yamashita and T. Kameda, Electing a Leader when Procesor Identity Numbers are not Distinct, Proc. *3rd Workshop on Distributed Algorithms*, WDAG 1989, 303–314.

[42] M. Yamashita and T. Kameda, Computing on Anonymous Networks: Part I - Characterizing the Solvable Cases, IEEE Trans. Parallel and Distributed Systems 7, 1996, 69–89.